Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/050727

International filing date: 18 February 2005 (18.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0404922.7
Filing date: 04 March 2004 (04.03.2004)

Date of receipt at the International Bureau: 01 July 2005 (01.07.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 23 June 2005

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

05MAR04 E878434-1 002094
P01/7700 0.00-0404922.7 NONE

Request for grant of a patent

THE PATENT OFFICE
D
- 4 MAR 2004
LONDON

1/77

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference — SLG/45349GB1

2. Patent application number — 0404922.7

- 4 MAR 2004

3. Full name, address and post code of the or each applicant

Dione plc
Dione House
Oxford Road
Stokenchurch
High Wycombe HP14 3SX

Patents ADP number — 7829021002

If the applicant is a corporate body, give the country/state of its incorporation — United Kingdom

4. Title of the invention — Secure Card Reader

5. Name of your agent

VENNER, SHIPLEY & CO

"Address for service" in the United Kingdom to which all correspondence should be sent

20 LITTLE BRITAIN
LONDON
EC1A 7DH

Patents ADP — 1669004

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or each of these earlier applications and the or each application number

Country	Priority application number	Date of filing

7. If this application is divided or otherwise derived from an earlier UK application, give the number and filing date of the earlier application

Number of earlier application	Date of Filing

Patents Form 1/77

8:	a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'YES' if:* *a) any applicant in 3. above is not an inventor, or* *b) there is an inventor who is not named as an applicant, or* *c) any named applicant is a corporate body)*	YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	10
Claim(s)	4
Abstract	1
Drawing(s)	10 & 10

10. If you are also filing any of the following state how many against each item.

Priority documents	N/A
Translations of priority documents	N/A
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents	

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 4 March 2004

12. Name and daytime telephone number of person to contact in the United Kingdom

Stuart Geary
020 7600 4212

Secure Card Reader

Description

The present invention relates to a secure card reader and, more particularly, to various security features that may be employed individually or in combinations.

Card readers for reading credit cards or the like are a familiar feature of modern life. In order for commerce to proceed using such devices, the devices must be secure so that they cannot be manipulated to facilitate fraudulent transactions.

According to a first aspect of the present invention, there is provided an enclosure comprising at least one tamper detection conductive path embedded therein, the conductive path or paths extending across the whole of the enclosure such that such that cutting through the enclosure, to make electrical contact with an element in the enclosure, without breaking or grounding an embedded conductive path is substantially impractical. Thus, any attempt to introduce a probe through the enclosure will be detectable because a hole sufficiently large to receive a probe would interrupt a sensing current flowing though a tamper detection conductive path.

The conductive path or paths are arranged in a plurality of layers such that conductors in different layers are offset relative to each other. Thus, the inevitable gaps, albeit small ones, between tracks in one layer are blocked by tracks in another layer.

Conveniently, the enclosure may be assembled from a plurality of printed circuit boards. Preferably, a plurality of said printed circuit boards are electrically connected. Thus, a single tamper detection current can extend across a plurality of printed circuit boards. A plurality of printed circuit boards may be connected by an interlocking mechanical joint, such as a halving joint or a dovetail joint.

According to a second aspect of the present invention, there is provided an apparatus comprising an electronic circuit covered by an enclosure according to the present invention.

The electronic circuit preferably comprises means for feeding current through each conductive path and detecting interruptions thereof.

The electronic circuit may comprise a multi-layer printed circuit board having a first face, covered by the enclosure, on which components are mounted, a second face on which no components are mounted. In this case, the conductors carrying signals between said components are separated from the second face by a tamper detection conductor path. This can prevent the signal path being probed through a hole from the second face.

According to a third aspect of the present invention, there is provided an apparatus comprising a housing member and an enclosure fixed in the housing member by a potting material, wherein the enclosure includes holes into which the potting material extends.

The enclosure need not be completely closed, e.g. a closed box, and may have an opening on one side which is covered by the housing member. In this case, the holes are provided around the rim of the opening. Preferably, the housing member includes a channel receiving at least part of the rim of the opening.

The holes are preferably through holes.

According to a fourth aspect of the present invention, there is provided an apparatus comprising;

a first housing shell having holes;

a second housing shell press-fitted to the first shell; and

a keypad membrane located in the first shell such that its keys extend through said holes,

wherein a wall is provided in the first or second shell to form a barrier between the seam between the shells and the membrane.

According to a fifth aspect of the present invention, there is provided an apparatus having a wall with an aperture in it, wherein at least one tamper detection conductor path is embedded in said wall around the aperture such that the aperture cannot be significantly enlarged without breaking an embedded tamper detection conductor path. This prevents the aperture being enlarged to prevent, for example, modified credit cards carrying signal probes being inserted through an enlarged slot.

According to a sixth aspect of the present invention, there is also provided a chip card contact module comprising a plurality of conductors leading from respective contacts, wherein none of the conductors leads from a contact in a direction opposite to any other. Consequently, the module can be arranged such that none of the conductors extends towards a card insertion slot, thereby making it more difficult for signals in the conductors to be sensed by inserting probes through the card slot.

Preferably, none of said conductors leads from a contact towards a card input side. More preferably, the contacts are arranged in two rows comprising a front row and a back row, the front row being nearer the card input side than is the back row. Still more preferably, the conductors from the back row lead directly away from the card input side and the conductors from the front row diverge and then lead directly away from the card input slot.

According to a seventh aspect of the present invention, there is provided an apparatus including tamper detection means, a memory and means responsive to the tamper detection means to replace data stored in the memory in the event of detection of tampering by the tamper detection means.

The apparatus may include switching means and the means responsive to the tamper detection means may be configured for closing the switching means so as to ground

a power supply terminal of the memory and thereby drain residual charge from the memory.

The foregoing aspects of the present invention may be employed in a card reader either individually or in combination. Preferably, all aspects are used together.

An embodiment of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a front view of a card reader module according to the present invention;

Figure 2 is an exploded view of the card reader shown in Figure 1;

Figure 3 is cross-section, somewhat exaggerated for clarity, of part of the PCB shown in Figure 2;

Figures 4(a) to 4(d) show, somewhat exaggerated for clarity, the tamper detection layers of the PCB shown in Figure 3;

Figure 5 is an exploded view of the cover shown in Figure 2;

Figure 6 shows a detail of the cover mounted to the front main member of the module shown in Figure 1 without potting material;

Figure 7 shows potting material holding the cover in place;

Figure 8 shows the keypad membrane installed on the front main member of the module shown in Figure 1;

Figure 9 shows part of the front face of the first PCB in Figure 2;

Figure 10 shows the keypad membrane;

Figure 11 is a cross-section of the module of Figure 1 along the line AA;

Figures 12(a) and 12(b) are respectively front and top views of the chip card contact module used in the card reader module shown in Figure 1; and

Figure 13 is a block diagram of the tamper detection circuitry of the card reader of Figure 1.

Referring to Figure 1, a card reader 1 comprises a body 2. A window 4, revealing an LCD panel, is located in to top half of the body 2 and the keys 5 of a keypad are distributed below the window 4. A card insertion slot 6 opens at the foot of the reader and chip cards can be inserted lengthways upwards into the slot 6 for reading.

Referring to Figure 2, the body 2 comprises a front and back main members 2a, 2b. The front and back main members 2a, 2d are coupled together by screws (not shown). The window 4 is incorporated into a bezel member 2c which is screwed to the front of the front main member 2a through PCB 8, thereby preventing removal of the window 4 when the module has been assembled.

The back main member 2d may be dispensed with and the front main member 2a fixed to another apparatus, which itself prevents access to the internals of the card reader 1 from behind.

A keypad membrane 7, a PCB 8, a cover 9 (shown exploded) are sandwiched with the keypad membrane 7 at the front and the cover 9 at the back. The keypad membrane 7 includes keys 5 which project through corresponding holes 33 in the front main member 2a. The PCB 8 is attached to the front main member 2a by screws 11 so that the keypad member 7 is located between the PCB 8 and the front main member 2a. The cover 9 is assembled from multi-layer PCBs and its sidewalls 9a, 9b are received in channels 15 formed by walls projecting from the back of the front main member 2a. The cover 9 completely covers the PCB 8 such that the only access to the PCB 8 is through a card entry slot 9c in a first end wall 9d.
Referring to Figures 3 and 4(a) to 4(d), the PCB 8 is a multi-layer PCB. The keypad side of the PCB 8 contains tracks 30 forming the fixed contacts of the keys. Above the key contact tracks 30 are four layers containing serpentine tracks 18a, 18b, 18c, 18d. These serpentine conductive tracks 18a, 18b, 18c, 18d are offset with respect to each other and arranged so that active signal paths 19 in other layers cannot be reached without breaking one of the serpentine tracks 18a, 18b, 18c, 18d and interrupting a monitoring current flowing therethrough. The loops of the serpentine tracks 18a, 18b, 18c, 18d are packed as close as is practicable.

Referring to Figure 5, the cover 9 comprises first and second side walls 9a, 9b, first and second end walls 9c, 9d and a roof 9f. Each of the side walls 9a, 9b, the end walls 9d, 9e and the roof 9f is made from multi-layer PCB and contains mutually off-set and cross-crossing serpentine conductive tracks like those of the PCB 8 and

shown exaggeratedly in Figures 4(a) to 4(d). The serpentine tracks are configured to make it impossible to drill through the cover without breaking one of the paths. The loops of the serpentine tracks are packed as close as is practicable. A complete conductive sheet (not shown), forming a ground plane, is included on the outside of the serpentine paths to prevent visual inspection of the tracking layers beneath, to act as a grounding contact if a metal drill is used to attack the serpentine tracks and also acts to reduce electromagnetic emissions from the assembly. Additionally, there is the possibility that a tool being using in an attempt to probe through the cover 9 will short a serpentine track 18a, 18b, 18c, 18d to the ground plane.

The ends of the side walls 9a, 9b and the first end wall 9e have notches. The notches enable the first end wall 9e to be connected to the side walls 9a, 9b by halving joints. The second end wall 9d has short tabs at either end which are received in the remaining notches in the first and second side walls 9a, 9b.

The roof 9f is rectangular and has a shallow notch in one end. This notch receives a short tongue, that projects from the top of the first end wall 9d, to locate the roof 9f.

The elements 9a, 9b, 9d, 9e, 9f of the cover 9 are held together by solder joints which also serve to interconnect the serpentine conductive paths in the different elements 9a, 9b, 9d, 9e, 9f.

The serpentine tracks in the cover are connected to the PCB 8 via a connector, comprising a part 10 located centrally on the PCB 8 which mates with another part (not shown) located centrally on the underside of the roof 9f.. Electrical connection is only made by the connector when the male part is fully inserted into the female part. This prevents removal of the cover 9 from PCB 8 without breaking the tamper detection circuit. The connector is completely enclosed by the cover 9

A slot 9c just large enough to allow a credit card to pass lengthwise is provided in the second end wall 9d. The second end wall 9d includes embedded conductors up

to the edge of the slot 9c such that the slot 9c cannot be enlarged without breaking a conductor.

The side walls 9a, 9b and the second end wall 9d each have a line of small through holes 20 in their lower margins, i.e. the parts received in the channels 15 formed on the back of the front main member 2a.

Referring to Figure 6, when the cover 9 has been located over the PCB 8, its side walls 9a, 9b and the second end wall 9d are received in the channels 15 such that the through holes 20 are within the channels 15.

Referring to Figure 7, the cover 9 is secured in position by an epoxy potting material 21. The potting material 21 extends into the through holes 20 locking the cover 9 in position.

Referring to Figure 8, the inner walls 16 of the channels 15 project upward beyond the installed keypad membrane 7 to form a barrier preventing probes being inserted sideways under the keypad membrane 7.

Referring to Figure 9, the front face of the first PCB is provided with a conductor pattern comprising first and second sets of pairs of interdigitated contacts 30, 31.

Referring to Figure 10, the key pad membrane 7 is moulded from an elastomeric material. A recess 32 is formed under each key 5 and carbon pills 34 are mounted in the recesses 32. Additional carbon pills 35 are distributed in non-recessed parts of the keypad membrane 7.

When the PCB 8 is installed behind the keypad membrane 7, the carbon pills 34 in the recesses 32 are aligned with the contact pairs 30 of the first set and are shorted only when keys 5 are pressed to produce user input signals. The other carbon pills 35 are aligned with the contact pairs 31 of the second set. The contact pairs of the second set are shorted by default. Thus, the circuitry on the PCB 8 can detect

attempts to probe behind the membrane by detecting an interruption in a current flowing through the contact pairs 31 of the second set.

Referring to Figure 11, the front main member 2a has a plurality of pillars 37 that project backwards between the holes. These pillars 37 are received by blind holes 38 in the keypad membrane 7 to press it towards the PCB 8. The blind holes 38 are aligned with the carbon pills 35, associated with the contact pairs 31 of the second set, and ensure that these contacts remain shorted during normal use.

Referring to Figures 12(a) and 12(b), a chip card contact module 40 is mounted on the PCB 8. The module 40 has a slot 41 that can receive a card inserted through the second slot 6 and slot 9c. A set of contacts 42 is arranged to make contact with the contacts of a properly inserted card. The contacts 42 are arranged in two rows 42a, 42b of four. The rear row 42a, i.e. the row furthest from the second slot 6, comprises the ends of four conductors 43, 44, 45, 46 that extend straight back away from the second slot 6. The front row 42b comprises the ends of four conductors 47, 48, 48, 50 which also extend back away from the second slot 6. However, these conductors 47, 48, 48, 50 jink sideways so that two extend straight back on each side of the conductors 43, 44, 45, 46 from the first row 42a of contacts.

Referring to Figure 13, the card reader has three distinct tamper detection system. These comprise the serpentine tracks 18a, 18b, 18c, 18d and associated circuitry, the additional carbon pills 35 and associated circuitry, and a temperature sensor 51 located within the cover 9, and associated circuitry.

A small battery 52, located within the cover 9, provides a permanent supply of power for the tamper detection circuitry.

The serpentine tracks 18a, 18b, 18c, 18d are connected in series between first and second resistors 53, 56. The first resistor 53 is connected to the positive terminal of the battery 52. The second resistor 56 is connected to ground. The node formed by the first resistor 53 and the serpentine tracks 18a, 18b, 18c, 18d is also connected to a first input of a window comparator 54. A second input of the window

comparator 54 is provided with a first reference voltage Vref1a, which is derived from the voltage across the battery 52, and a third input of the window comparator 54 is provided with a second reference voltage Vref1b, which is derived from the voltage across the battery 52.

Under normal conditions, the first input of the window comparator 54 is between the first and second reference voltages Vref1a, Vref1b and the output of the first comparator 54 is low. However, if one of the serpentine tracks 18a, 18b, 18c, 18d is broken, the voltage on the first input of the window comparator 54 rises past the first reference voltage Vref1a, causing the output of the window comparator 54 to go high. Similarly, if one of the serpentine tracks 18a, 18b, 18c, 18d is grounded, the voltage on the first input of the window comparator 54 falls past the second reference voltage Vref1b, causing the output of the window comparator 54 to go high.

A first latch 55 latches the high state of the output of the window comparator 54 so that even fleeting disturbances of the current through the serpentine tracks 18a, 18b, 18c, 18d can be responded to reliably.

The carbon pills 35 and associated contact pairs 31 are connected in series between a pull-up resistor 57. The node formed by the pull-up resistor 57 and current path through the carbon pills 35 and associated contact pairs is also connected to a first input of a first comparator 58 A second input of the first comparator 58 is provided with a third reference voltage Vref2, which is derived from the voltage across the battery 52.

Under normal conditions, the first input of the first comparator 58 is low and the output of the first comparator 58 is also low. However, if the keypad membrane 7 is lifted, separating a carbon pill 35 from the associated contacts 31, the voltage at the first input of the first comparator 58 rises past the third reference voltage Vref2 and the output of the second comparator 58 then goes high. A second latch 59 latches the high state of the output of the first comparator 58 so that even a fleeting lifting of part of the keypad membrane 7 can be reliable responded to.

The output of the temperature sensor 51 is connected to a first input of a second comparator 62. The other input of the second comparator 62 is provided with a fourth reference voltage Vref3, which is derived from the voltage across the battery 52.

Under normal conditions, the output of the second comparator 62 is low. However, if the temperature, sensed by the temperature sensor 51 falls below –25°, which indicates cooling being used to slow the response of other tamper detection systems, the output of the second comparator 68 goes high and is latched by a third latch 63.

The outputs of the latches 55, 59, 63 are supplied to concentrating circuit 65, e.g. an AND-gate, which produces an erase signal when the outputs of any one or more of the latches 55, 59, 63 is high.

The erase signal is fed to an erase circuit 67 which is responsible for zeroisation of the security module's memory 69. In response to the erase signal, the erase circuit 67 write zero to every location in the memory 69 and then opens a first switch 71 to remove power from the memory 69. Finally, a second switch 72 is closed to remove any residual charge from the memory 69.

It will be appreciated that the security features described above may be used in other combination both with each other and with other security features not described herein.

Claims

1. An enclosure comprising at least one tamper detection conductive path embedded therein, the conductive path or paths extending across the whole of the enclosure such that such that cutting through the enclosure, to make electrical contact with an element in the enclosure, without breaking or grounding an embedded conductive path, is substantially impractical.

2. An enclosure according to claim 1, wherein the conductive path or paths are arranged in a plurality of layers such that conductors in different layers are offset relative to each other.

3. An enclosure according to claim 1 or 2, assembled from a plurality of printed circuit boards.

4. An enclosure according to claim 3, wherein a plurality of said printed circuit boards are electrically connected.

5. An enclosure according to claim 3 or 4, wherein a plurality of said printed circuit boards are connected by an interlocking mechanical joint.

6. An apparatus comprising an electronic circuit covered by an enclosure according to any preceding claim.

7. An apparatus according to claim 6, wherein the electronic circuit comprises means for feeding current through each conductive path and detecting disturbances thereof.

8. An apparatus according to claim 6 or 7, wherein the electronic circuit comprises a multi-layer printed circuit board having a first face on which components are mounted, a second face on which no components are mounted.

9. An apparatus according to claim 8, wherein the conductors carrying signals between said components are separated from the second face by a tamper detection conductor path.

10. An apparatus comprising a housing member and an enclosure fixed in the housing member by a potting material, wherein the enclosure includes holes into which the potting material extends.

11. An apparatus according to claim 10, wherein the enclosure has an opening on one side and the opening is covered by a housing member.

12. An apparatus according to claim 11, wherein the holes are provided around the rim of the opening.

13. An apparatus according to claim 11 or 12, wherein the housing member includes a channel receiving at least part of the rim of the opening.

14. An apparatus according to any one of claims 10 to 13, wherein the holes are through holes.

15. An apparatus according to any one of claims 10 to 14, wherein the enclosure is an enclosure according to any one of claims 1 to 5.

16. An apparatus comprising;

a first housing shell having holes;

a second housing shell press-fitted to the first shell; and

a keypad membrane located in the first shell such that its keys extend through said holes,

wherein a wall is provided in the first or second shell to form a barrier between the seam between the shells and the membrane.

17. An apparatus according to claims 14 or 15 and claim 16, wherein said wall comprises a side of said channel.

18. An apparatus having a wall with an aperture in it, wherein at least one tamper detection conductor path is embedded in said wall around the aperture such that the aperture cannot be significantly enlarged without breaking an embedded tamper detection conductor path.

19. An apparatus according to claim 18 and any one of claims 6, 15, 16, 17, wherein said wall with an aperture in it is part of said enclosure.

20. A chip card contact module comprising a plurality of conductors leading from respective contacts, wherein none of the conductors leads from a contact in a direction opposite to any other.

21. A chip card contact module according to claim 20, having a card input side into which a card can be inserted for reading, wherein none of said conductors leads from a contact towards the card input side.

22. A chip card contact module according to claim 21, wherein the contacts are arranged in two rows comprising a front row and a back row, the front row being nearer the card input side than is the back row.

23. A chip card contact module according to claim 22, wherein the conductors from the back row lead directly away from the card input side and the conductors from the front row diverge and then lead directly away from the card input slot.

24. A card reader comprising an apparatus according to 19, wherein a chip card contact module according to any one of claims 20 to 23 is located in the enclosure for contacting the contacts on a card inserted through said slot in the enclosure.

25. An apparatus including tamper detection means, a memory and means responsive to the tamper detection means to replace data stored in the memory in the event of detection of tampering by the tamper detection means.

26. An apparatus according to claim 25, including switching means, wherein the means responsive to the tamper detection means is configured for closing the switching means so as to ground a power supply terminal of the memory and thereby drain residual charge from the memory.

5

27. An apparatus according to any one of claims 1 to 19 and claim 25 or 26.

28. A card reader according to claim 24 and claims 25 or 26.

Abstract

Secure Card Reader

A secure card reader includes several security measures. Access to the reader's main circuitry is prevented by an enclosure whose walls contain embedded conductive paths. Breaking or grounding of one of these paths can be detected electronically. A similar arrangement of conductive paths prevent enlarging of a card receiving slot. If tampering is detected using the embedded conductive paths, the reader's memory is wiped. The enclosure has apertures in its walls and is held in place by a potting material that extends into the apertures. Means is also provided to detect attempts to probe behind a keypad membrane. The contacts for the chip of a chip card are arranged so that their leads all extend away from the card insertion slot.

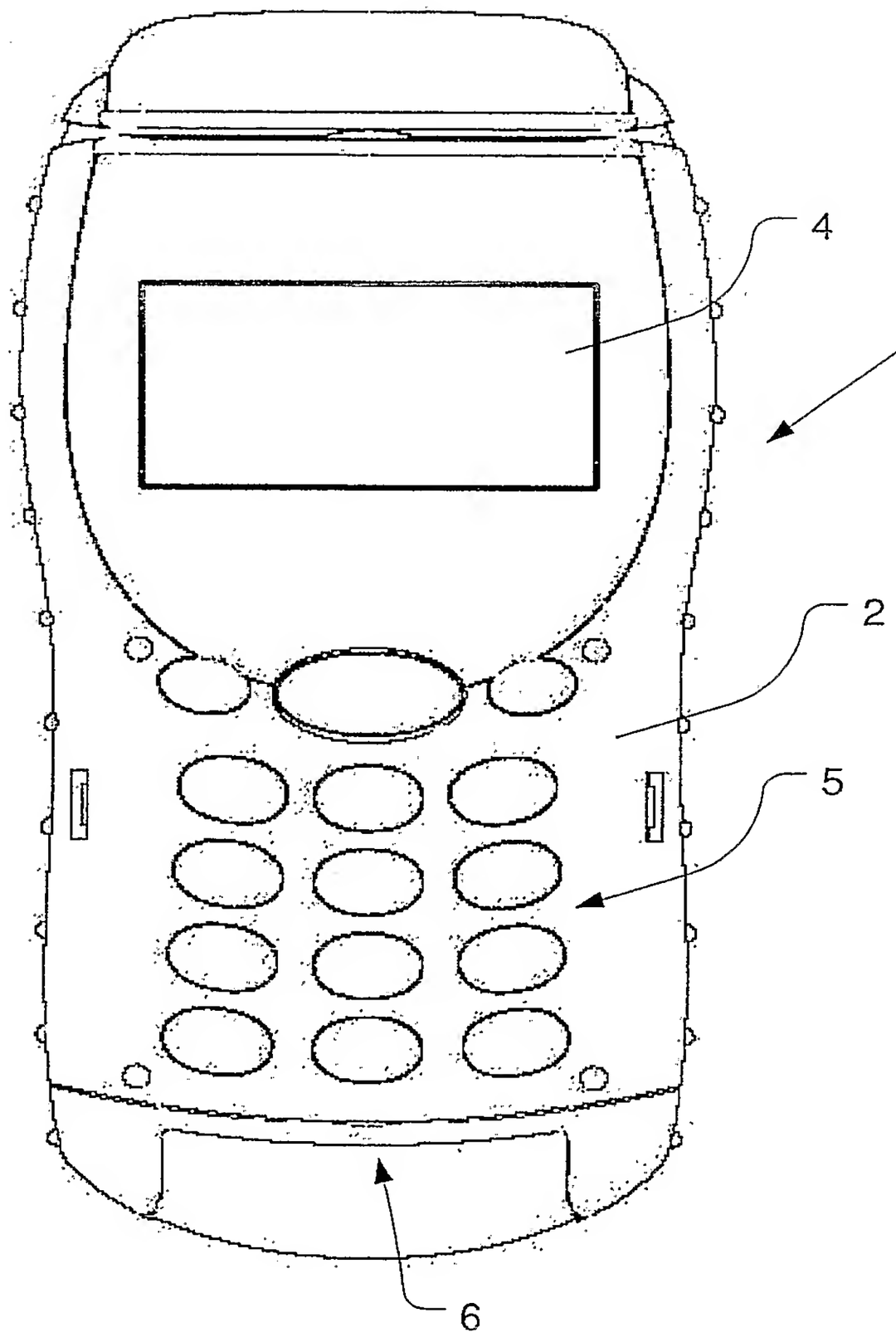


Figure 1

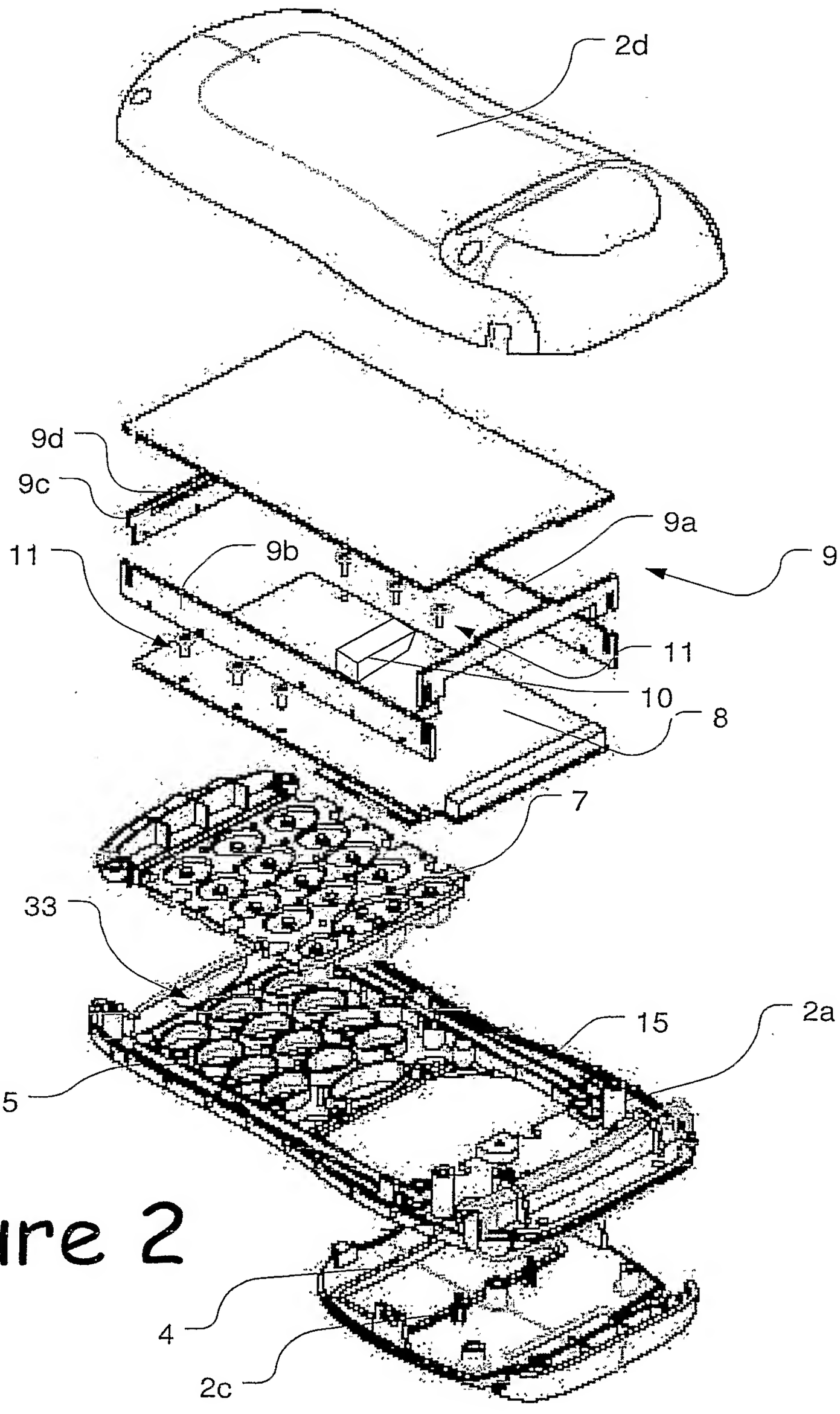


Figure 2

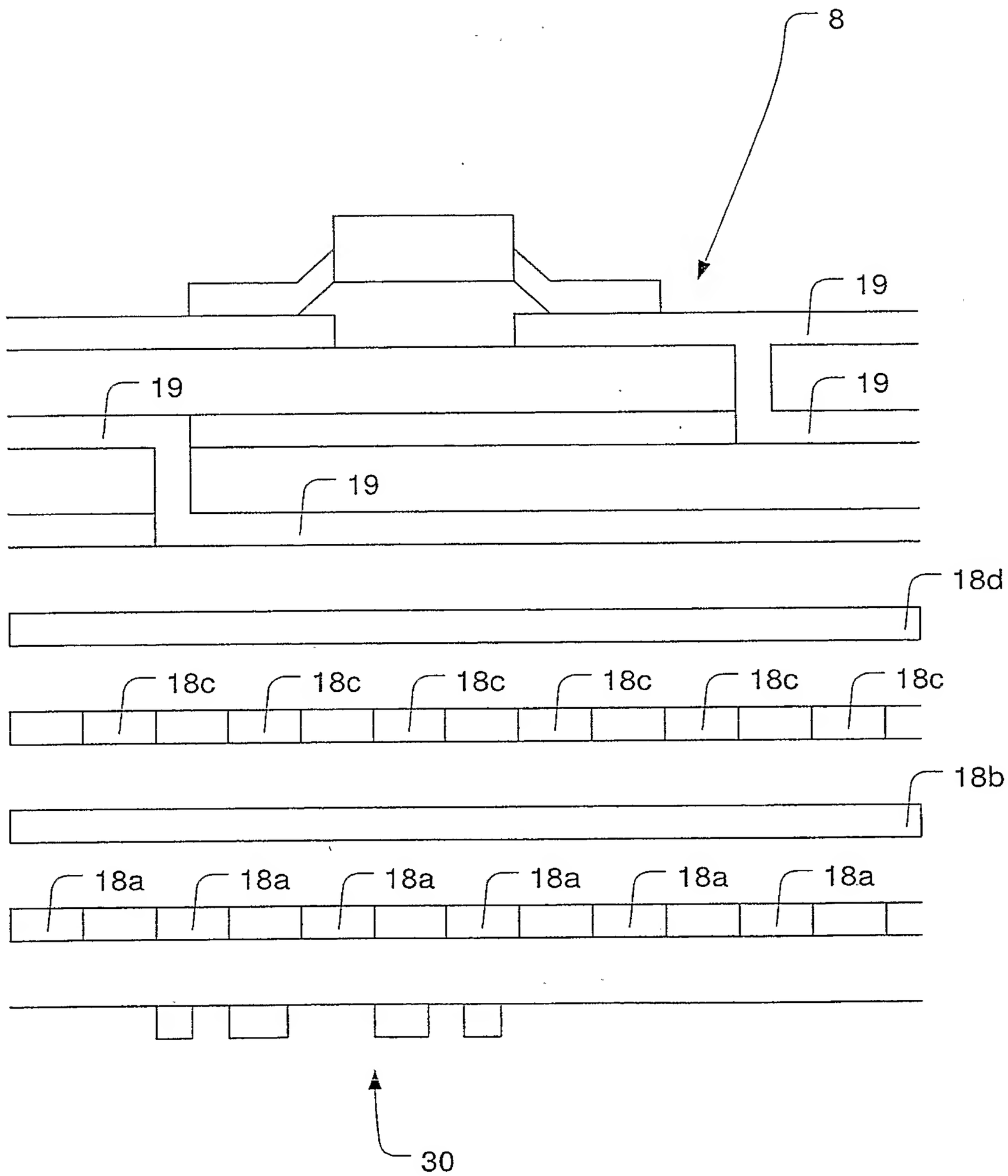

8
19
19
19
19
18d
18c
18c
18c
18c
18c
18c
18b
18a
18a
18a
18a
18a
18a
30

Figure 3

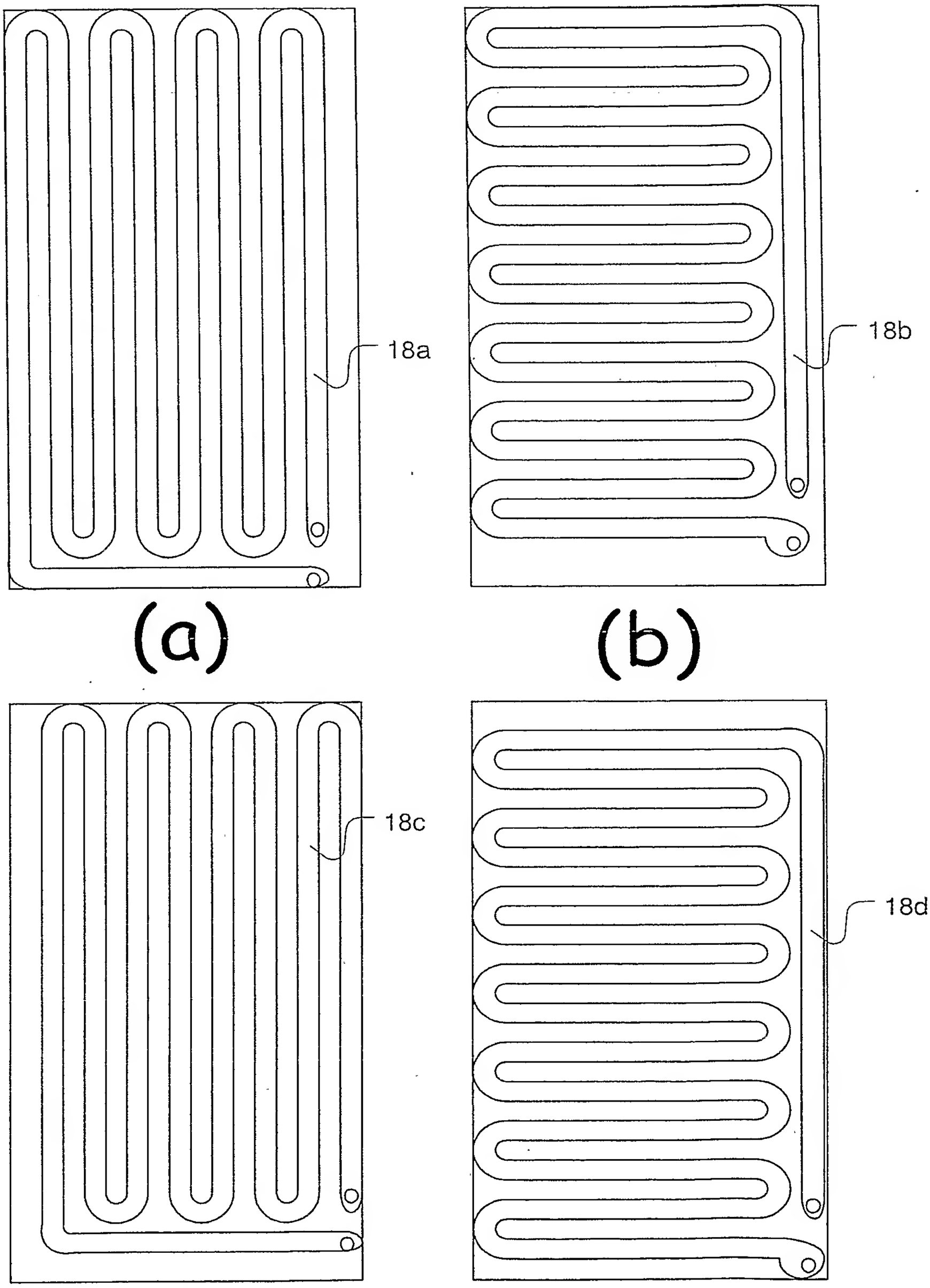


Figure 4

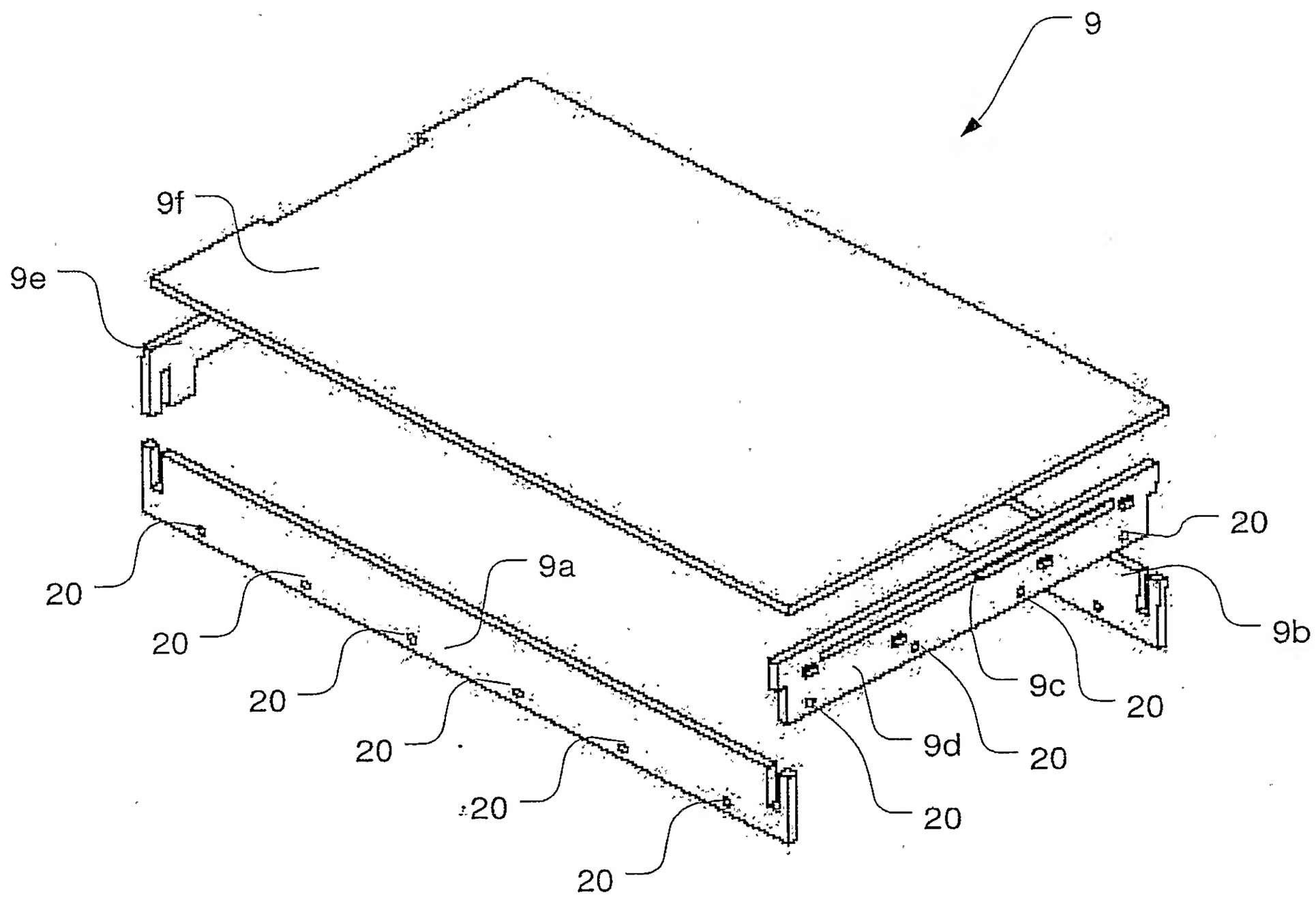


Figure 5

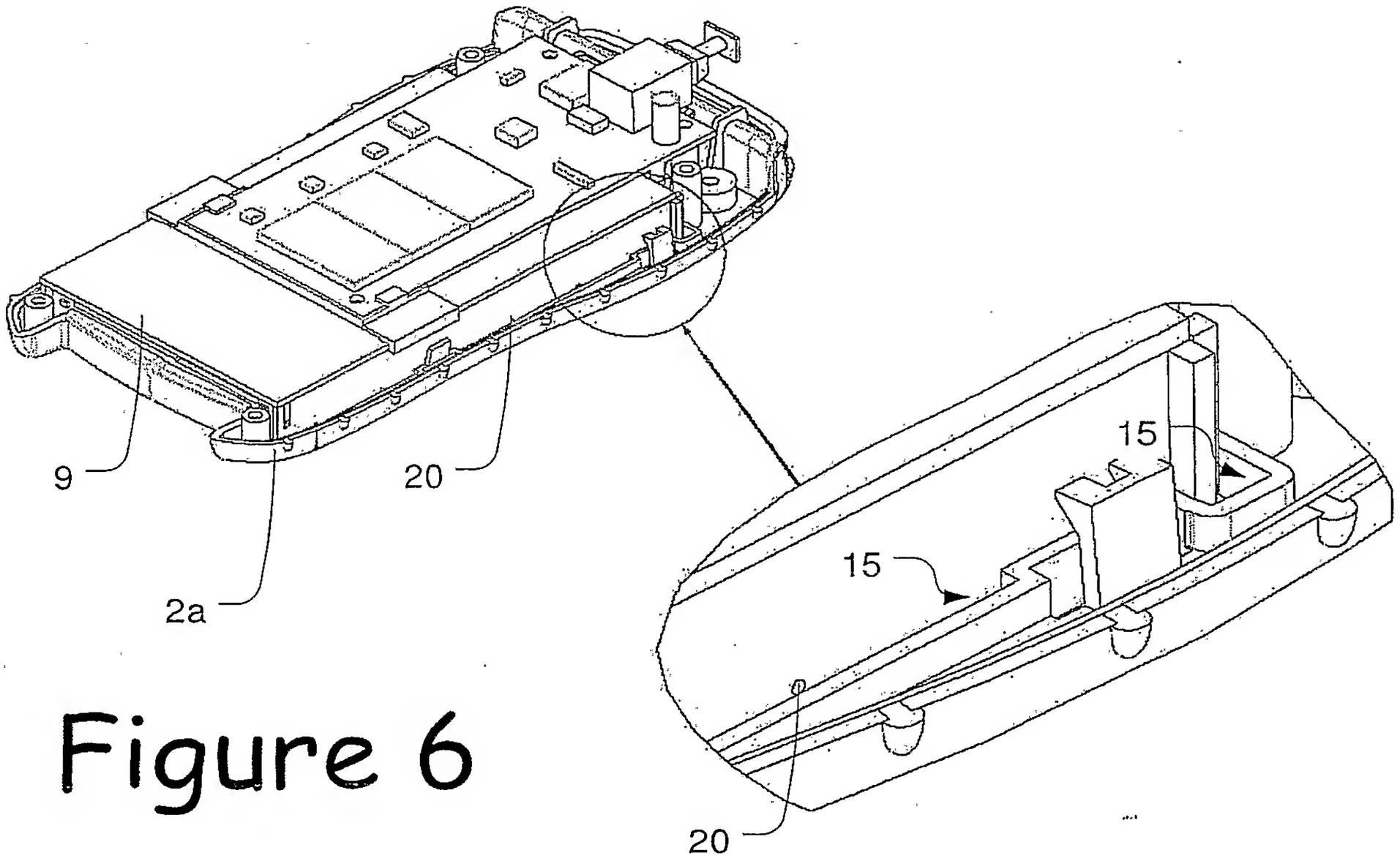


Figure 6

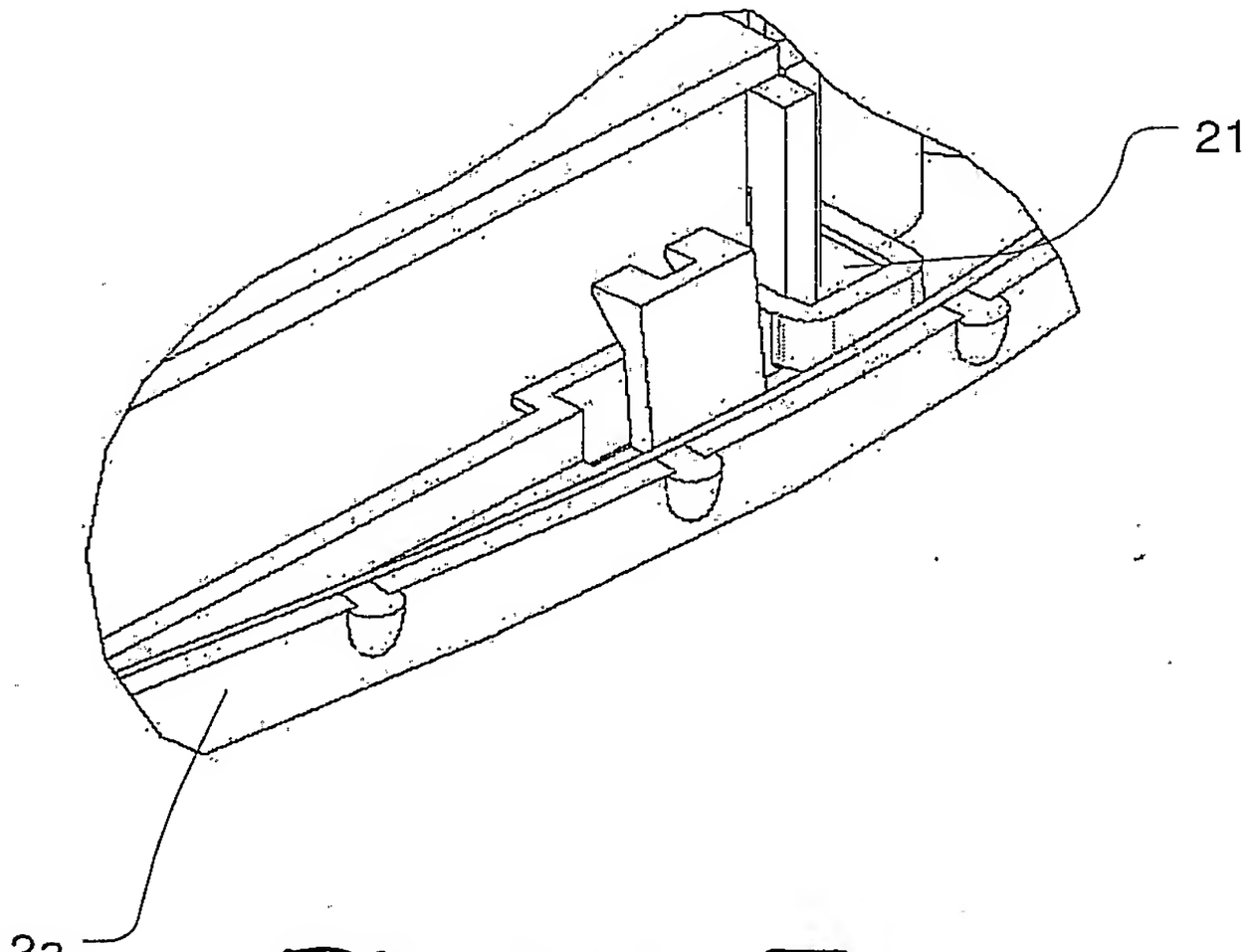


Figure 7

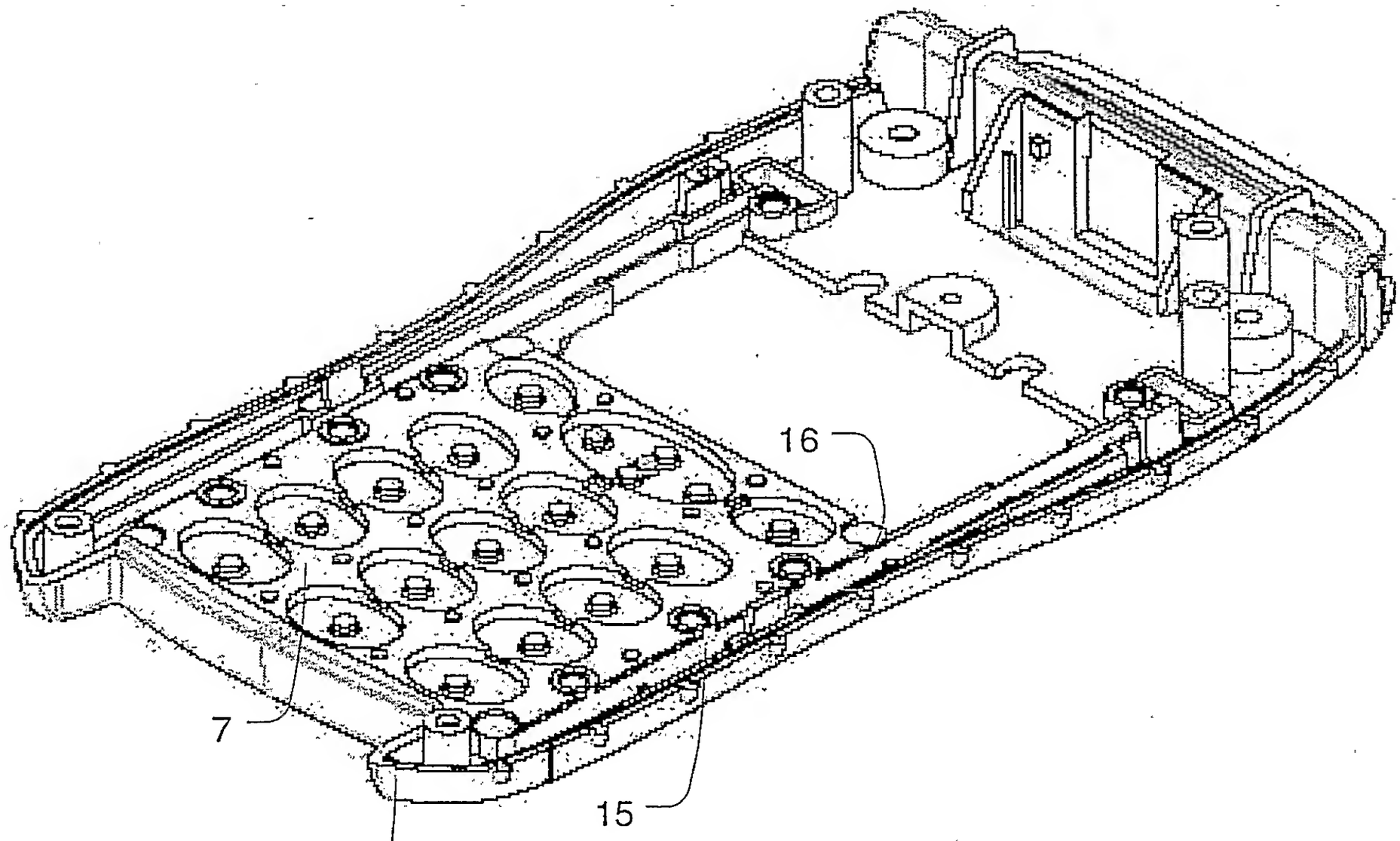


Figure 8

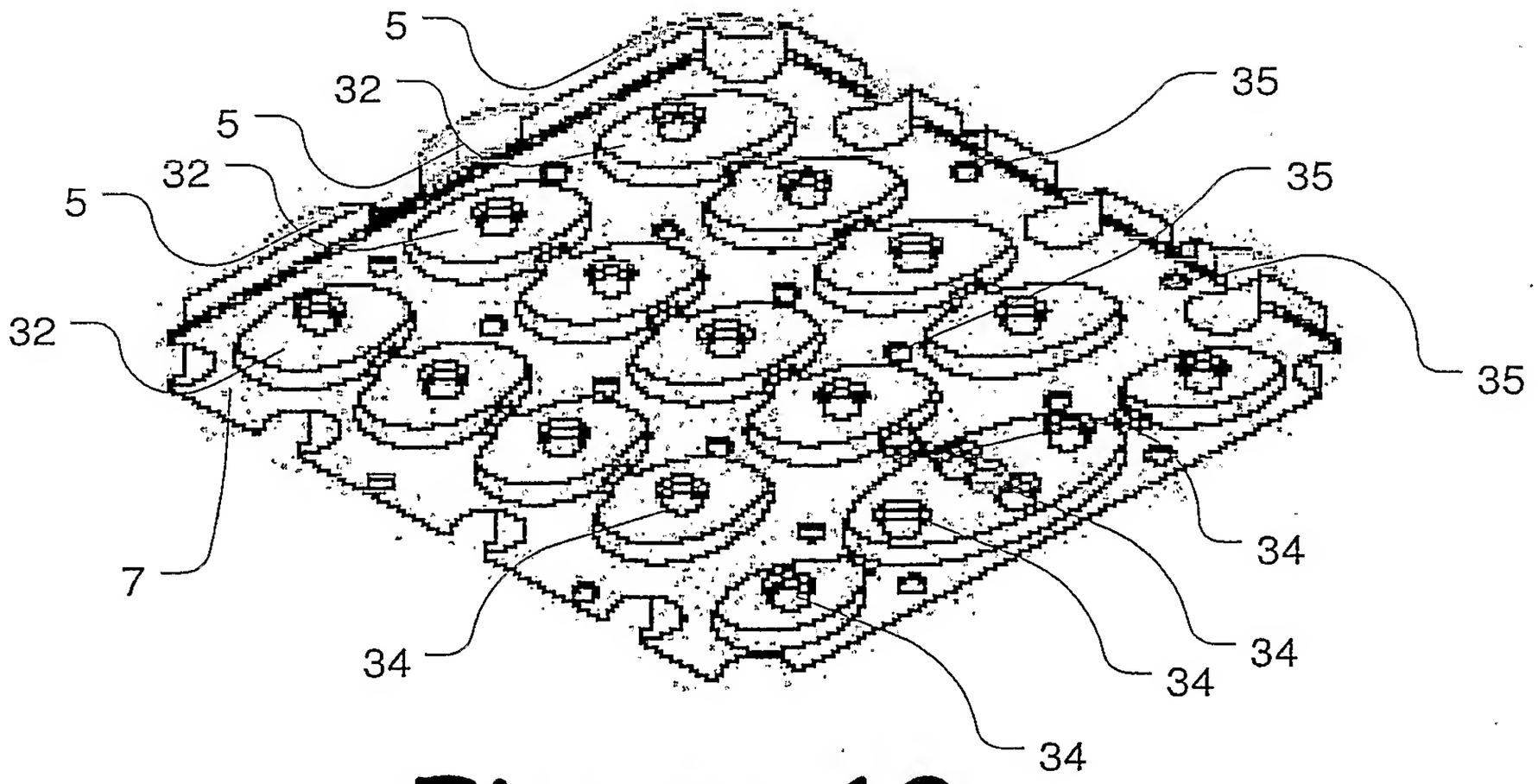
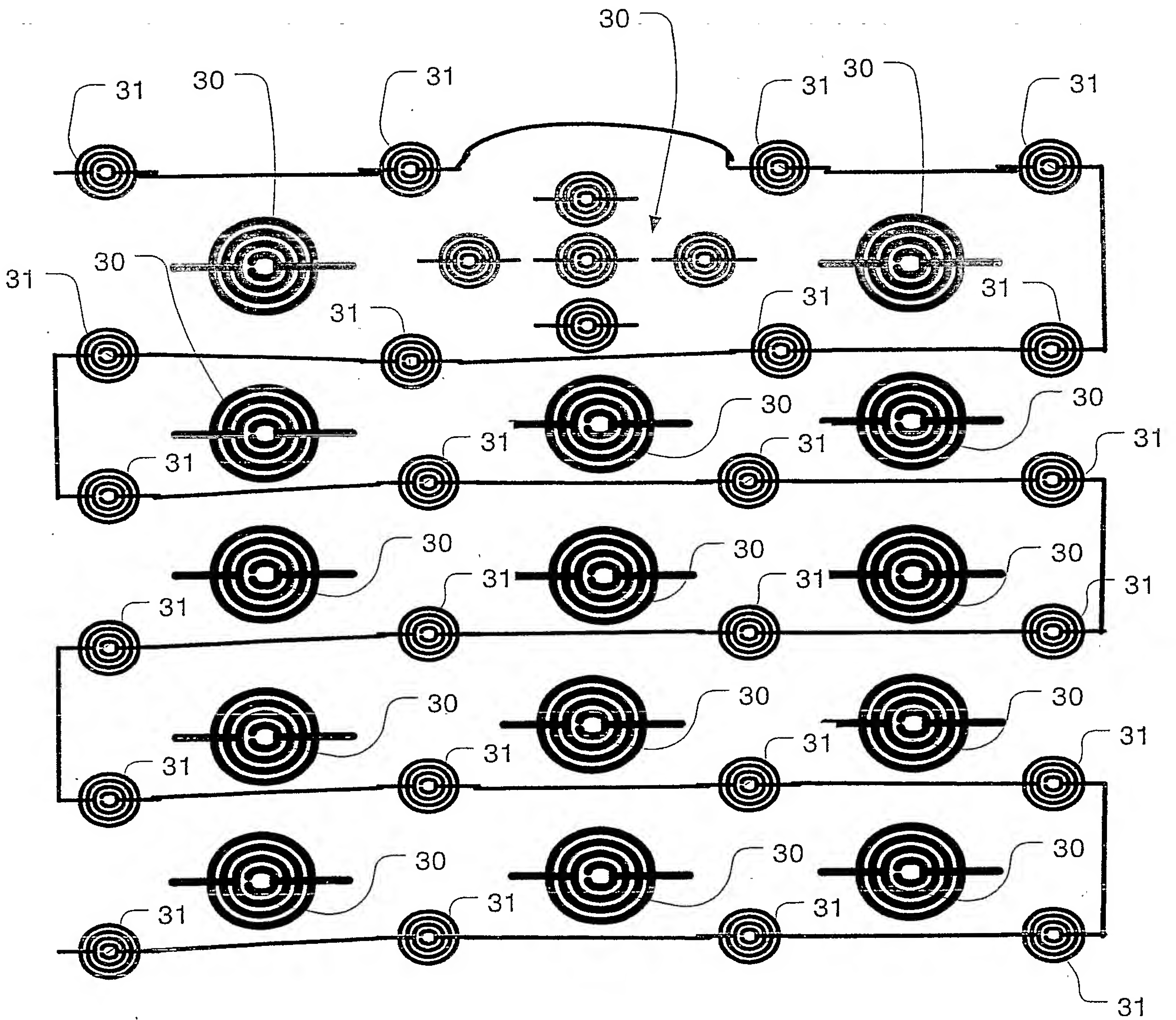


Figure 10



30
31
30
31
31
30
31
30
31
31
31
31
30
30
31
31
30
31
31
30
31
30
31
31
30
31
31
30
31
30
31
31
30
31
30
31
30
31
31
31
30
31
30
31
30
31
31

Figure 9

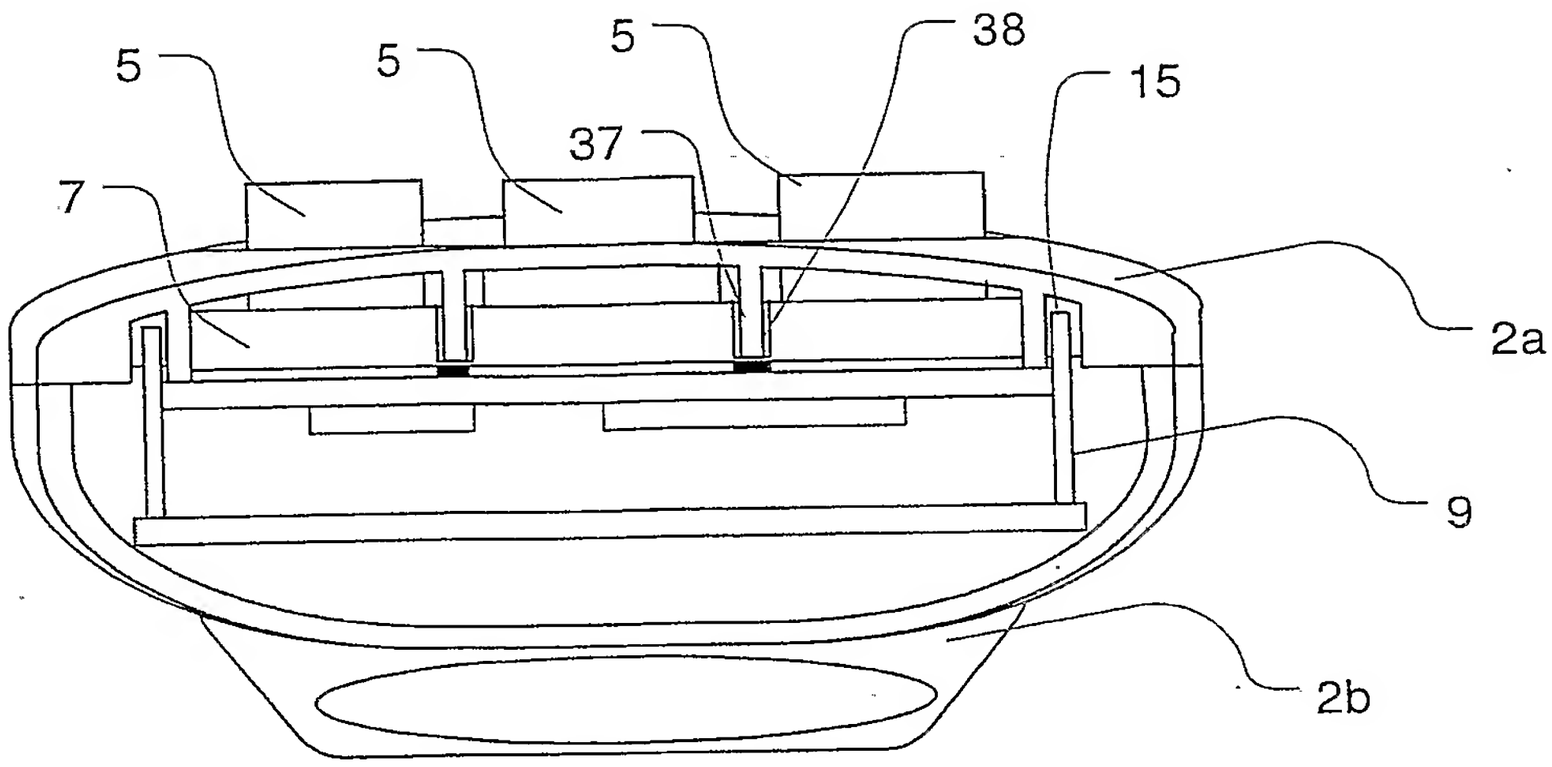


Figure 11

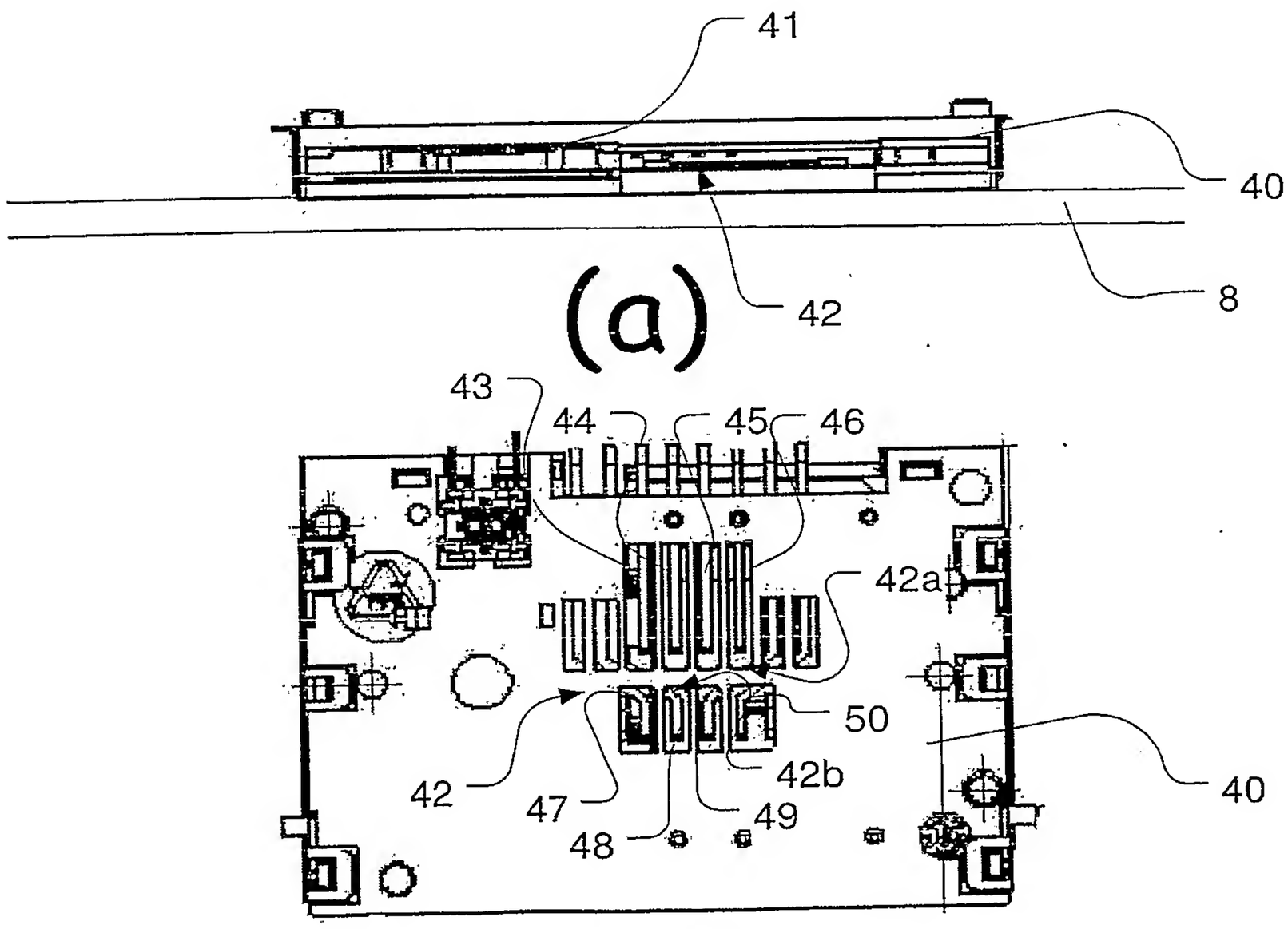


Figure 12

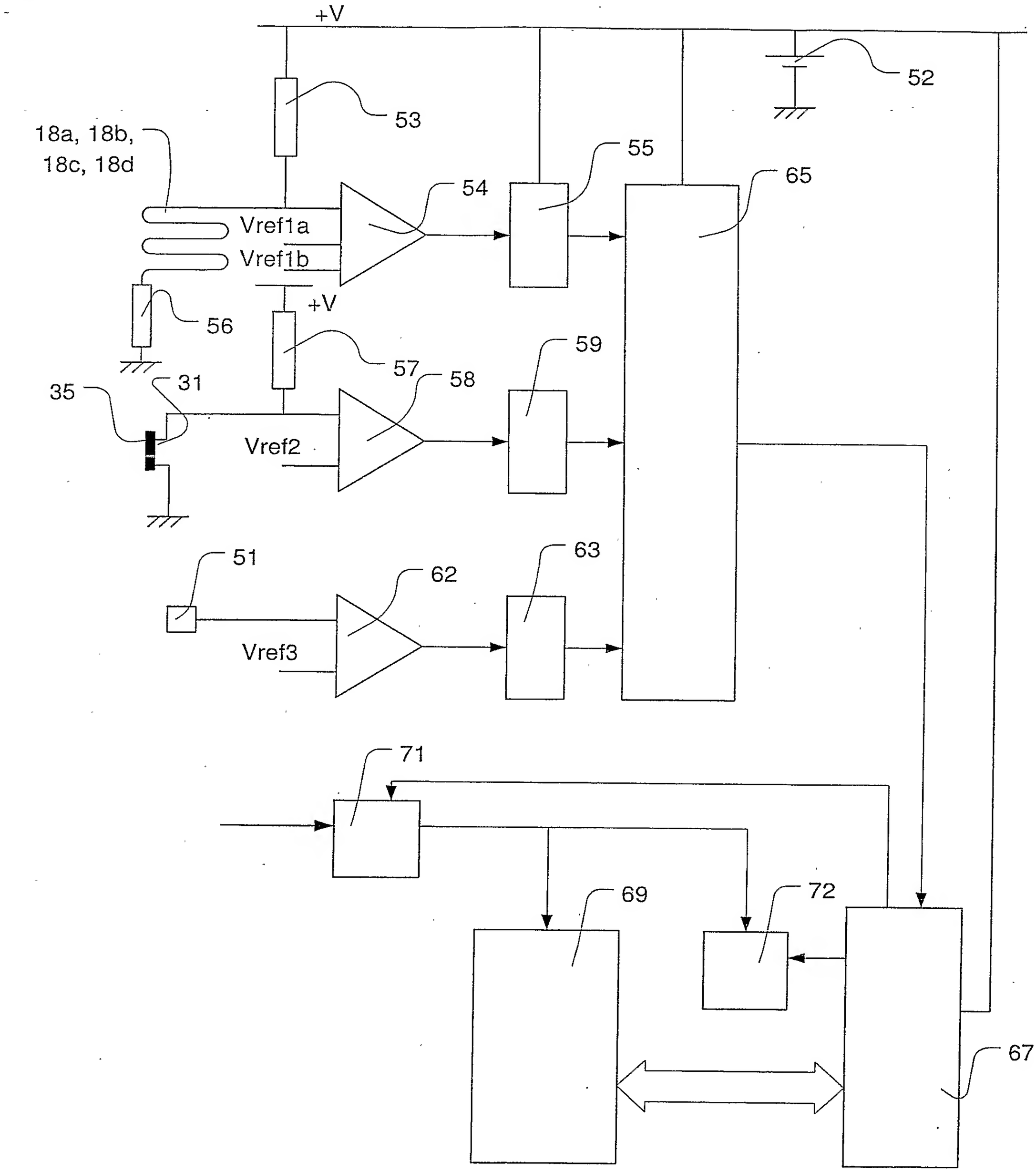

+V
52
53
18a, 18b,
18c, 18d
55
54
65
Vref1a
Vref1b
+V
56
59
57
58
35
31
Vref2
51
62
63
Vref3
71
69
72
67

Figure 13